放送における情報セキュリティ技術
Information Security in Broadcasting

難波　誠一
Seiichi　NAMBA

ＮＨＫ放送技術研究所
NHK Science and Technical Research Laboratories

１．まえがき

最近、放送における情報セキュリティ技術に関する話題が多くなっている。これは、衛星を使って広範囲に有料放送ができるようになり、技術方式を定めることが必要になったことが大きいが、受信者の視聴要求や送られる情報の多様化により、特定の人から料金を徴収して各種の放送サービスを行う必要性が増していることにもよっている。

特定の人のみに放送を行うためには、信号をスクランブルして送り、またこのスクランブル放送を制御するために種々の情報(関連情報と呼ばれる)を送り処理する技術が必要となる。有料放送は諸外国では既に行われている。我が国ではＣＡＴＶ等有線による放送では既に実施されているが、電波による放送では、郵政省の電気通信技術審議会(電通技審)や放送技術開発協議会(ＢＴＡ)で答申または審議が行われている段階である。審議対象の放送サービスとしては、放送衛星を用いたテレビジョン放送(答申済み)、ハイビジョン(高精細度テレビジョン)、通信衛星を用いたテレビジョン放送、音声放送(多チャンネルＰＣＭ音声放送)、地上波のテレビジョン多重ファクシミリ放送などがある。

ここでは、このような背景等について述べた後、システムの構成、その各要素における情報セキュリティ技術の具体的な内容等についてまとめる。

２．放送において情報セキュリティ技術が必要となる背景

放送のようなもともと多くの人に広く情報を伝える役割を担うシステムで情報セキュリティ技術が話題になる背景としては次のような点が挙げられる。

(1) 放送衛星による有料放送

放送衛星３号(ＢＳ－３)では、ＮＨＫの２チャンネルの他に民間放送が加わることになっており、その営業形態として広告放送の他に有料放送が行われることになっている。このため放送法が改正され、1988年11月に電通技審で答申された有料方式[1]によって放送が行われる予定である。

(2) スピルオーバーへの対策

放送信号をスクランブルする技術は受信地域を限定する目的でも利用される。目的とする地域以外にも電波が到達することによるスピルオーバーと呼ばれる現象は、直接放送衛星の出現によって極めて広い範囲にテレビ放送が可能となったことから、特にヨーロッパのように多数の国が隣接する場合に問題となり、この問題を解決するために使用される。

(3) 通信衛星による放送

通信衛星は直接放送衛星に比べ出力電力が低いがやや大きい受信アンテナを使用して、例えばＣＡＴＶのヘッドエンドへ向けて番組を供給するのに使用されている。この通信衛星による通信は特定の人を対象にしており、他の人が受信できないようにするためにスクランブルがかけられている。これは通信内容を秘匿する本来の目的での使い方と言える。しかし、この電波はやや大きいアンテナを用意すれば個人でも受信できることから、通信衛星を利用して不特定の受信者に向けて放送を行うことが考えられている。この場合は、一度にチャンネル数が増えることから、既存の放送に影響が考えられるので、異なる営業形態すなわちスクランブルをかけ有料放送とすることが必要とされる。

(4) 番組調達上の問題

衛星放送は受信できる範囲が極めて広いことから、番組供給業者は多額の番組放送料を要求するが、実際には受信者数は少ない場合がある。このとき、実際の受信者数を証明するために、スクランブルをか

け、受信を契約した人の数を明らかにする必要がある場合がある。

以上のように、種々の目的があるが、これら受信を限定する技術方式を限定受信(Conditional access)方式と呼び、広く検討が進められている。

3．限定受信システムの構成

現在、各種の放送サービスで限定受信が提案、実施されているが、CCIRでは、限定受信システムの基本的な構成を図1のように、信号をスクランブルする機能と各サービスへのアクセスを制御する機能とに分けて考え、これらをさらに具体化して図2の構成にまとめている。[1]実際のシステムではこれらの要素を全て必要とするわけではなく、一部を用いて実用されているものも多い。このレポートで挙げられているシステム例については文献(2)、(3)を参照されたい。

一般に限定受信システムは次のような条件を満たす必要がある。[2]

1) 不正な受信に対して安全性が高いこと。
2) 受信者には所要のサービスにアクセスする資格を与えることができること。
3) サービスにアクセスする方法として、種々の営業形態(フラットフィー、ペイパービュー等)を放送事業者が選択できること。
4) 多種のサービスに適用できるように共通部分を標準化して大量生産の効果を上げるとともに、秘密の部分はインターフェースのみを標準化した安全なモジュールの中に含め、管理と保守を簡単にできること。
5) スクランブル放送にともなう劣化、すなわち、a)スクランブル/デスクランブル処理による劣化、b)制御データの伝送誤りに伴なう劣化、c)限定受信の管理用データの伝送による伝送容量の損失、が少ないこと。

図3は我が国の衛星放送のスクランブル放送システム(以下、BS有料方式と呼ぶ)の構成例を示している。CCIRの図2の構成と類似しているが、説明及び比較の都合上再掲してある。

4．システム内の秘密要素と安全性

放送分野で暗号化を行う場合、放送番組自体は特に秘密を守る必要がないことが多い。従って、鍵が漏れても受信者の受ける損害が明確でなく、鍵管理の安全性が期待できない特徴がある。これは通常の秘密通信や経済活動等における暗号と大きく異なる点であり、放送で使用する暗号の鍵は通信の一方の当事者である受信者にも分らないようにする必要がある。その方法としては鍵を受信機等の中に収め、外から知られないようにするなどが考えられるが、完全に秘匿することは困難である。

図3のシステムにはいくつかの秘密要素が含まれているが、これらを安全性の観点でまとめると表1のようになる。ところで図3の中の秘密要素には次のような種類があることが分る。

(1) 技術内容が公開される部分

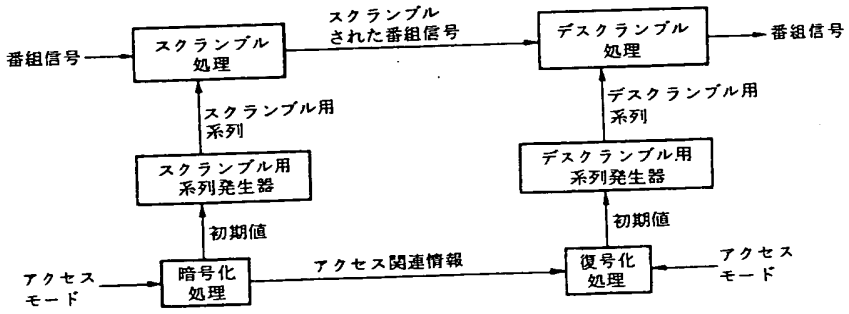


図1　限定受信システムの基本構成

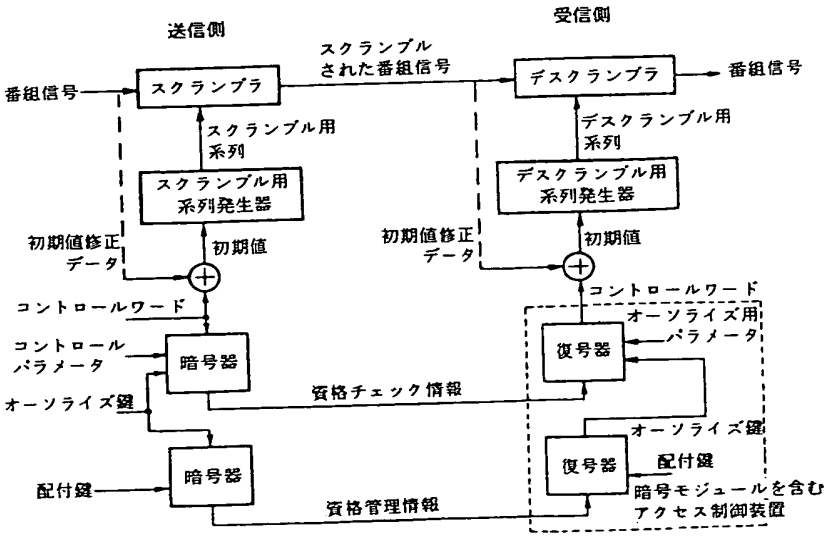
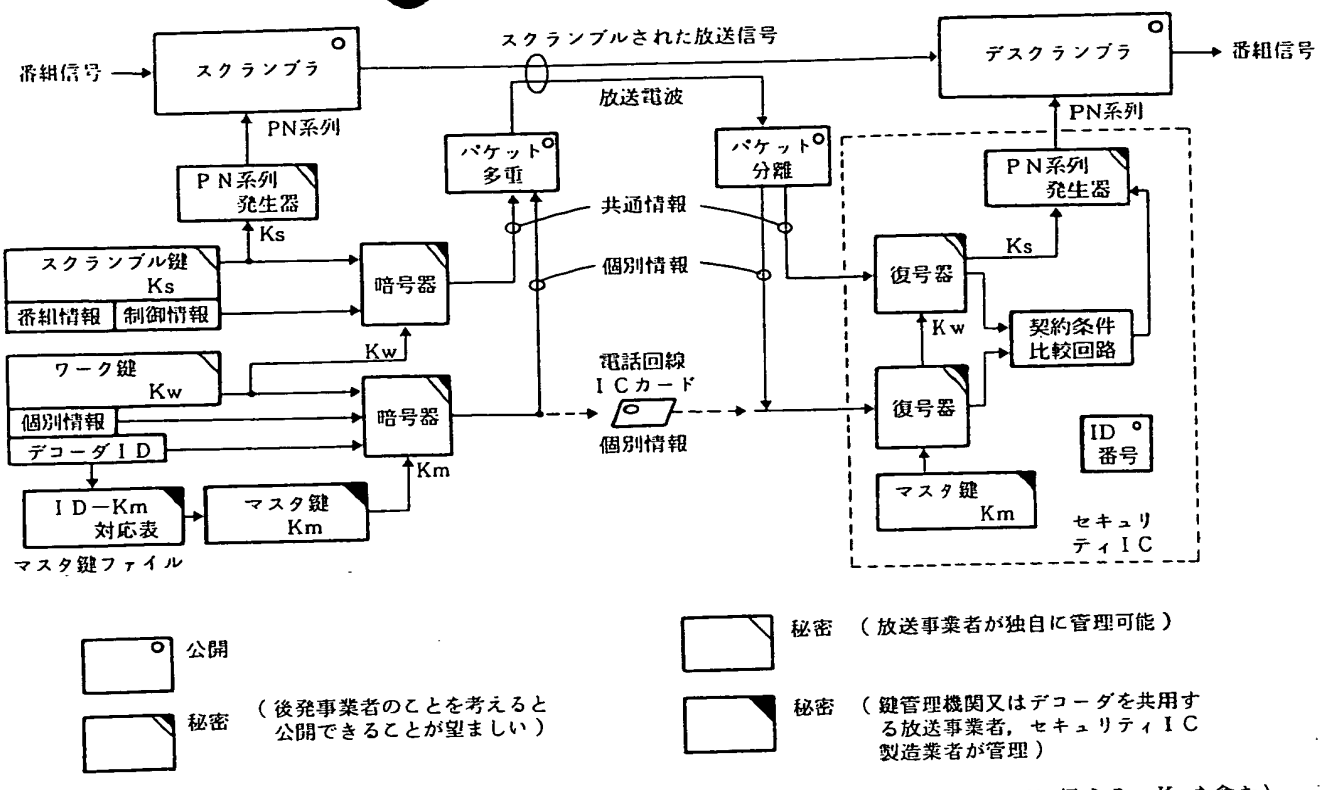


図2　限定受信システムの構成



関連情報
- 共通情報
  - 番組情報 （契約内容との照合等のために、番組の属性をデコーダに伝える。Ksを含む）
  - 制御情報 （特定のデコーダのデスクランブル機能を強制オフ/オンする）
- 個別情報 （契約内容を各デコーダに伝える。Kwを含む）

図3　スクランブル放送システムの構成

表1　スクランブル放送における秘密情報とその安全性

秘密要素の種類		受信機へ配付する方法	秘密を破る方法	安全性を得る方法		秘密要素の更新周期
				方法	暗号化する鍵	
スクランブル方式		受信機に組み込み（アルゴリズム固定）	スクランブルされた信号の性質を観測して方式を知る	パラメータを時間とともに変える	PN（疑似ランダム）系列	更新なし
PN系列		スクランブル鍵Ksをもとに受信機内で発生	スクランブルされた信号を解析して一周期分の系列を得る	PN系列の発生方法を時間とともに変える	スクランブル鍵 Ks(PN系列発生の初期値)	水平走査周期又は音声クロック周期
暗号化鍵	Ks（スクランブル鍵）	電波（Kwで暗号化）で送る	PN系列から推定する	非線形演算を入れ推定しにくくする		例えば、1秒
			伝送されるKsを窃用する	伝送される信号を暗号化する	ワーク鍵 Kw	
	Kw（ワーク鍵）	電波（Kmで暗号化）又はICカード、電話線等で送る	電波又はICカード等から知る	伝送される信号を暗号化する	マスタ鍵 Km	例えば、1月～1年
	Km（マスタ鍵）	有料デコーダユニット（受信機）の製造時に組み込み	鍵の情報を何等かの方法で得る	各デコーダのKmの情報を製造業者、放送事業者等で厳重に管理する		更新なし（デコーダの交換）
暗号方式		アルゴリズムは受信機に組み込み	・簡易な暗号の場合は送られる暗号化データを解析する ・何等かの方法で、製造業者、放送事業者等から情報を得る	・強力な暗号の場合は公開可能 ・弱い暗号の場合は管理を厳重にする		更新なし（ただし、関連情報のプロトコル番号を変えることにより暗号方式の更新が可能）

(a) スクランブラ、デスクランブラ

これらは非公開としても、放送電波の信号が解析されて、いずれは知られると考えられる。従って、公開しても良いように安全性を予め考慮しておく必要がある。

(b) パケット多重及び分離

関連情報を衛星放送の電波で送る場合、データチャンネル領域でパケットで伝送されることになっている。データチャンネルでは各種データサービスの信号も同時に送られることから、パケット構成は図4のように標準化されており、パケットの多重方法も定められている。[4]従って、関連情報の伝送位置を秘密にすることにより安全性を確保することは考えず、伝送される内容を暗号化することで安全性を保持している。

(2) 秘密とされるが、後発事業者のことを考えると公開できることが望ましい部分

(a) ＰＮ信号系列発生器

放送の場合は、複数の放送事業者が同じ受信機を使用することが原則となるので、ＰＮ系列発生器の構成が分らなければ、後発の放送事業者は事業が始められない。従って、後発の放送事業者が対等の立場で事業を開始できるためには、この情報は公開されていることが望ましく、公開に耐えられる方式を採用することが必要となる。例えば、ＥＢＵ(ヨーロッパ放送連合)のＭＡＣ/パケット方式[5]は多くの国、放送事業者で使用することが想定されているが、この仕様ではＰＮ系列発生器の詳細な回路が定められている。(６．参照)

(b) 暗号アルゴリズム及び暗号回路

これも(a)と同様である。ただし、この部分はＰＮ信号系列発生器に比べて低速で処理が可能で、ソフトウェアで対処しうる。また将来の変更にも対応できるようにする必要がある。従って、電通技審の答申でも放送事業者の選択に任せられており、特に定められていない。[1]

(3) 秘密であるが放送事業者が独自に管理可能な部分

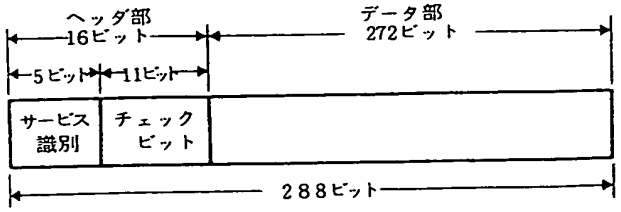


図４　パケットの構成

(a) K_s(スクランブル鍵)

これはＰＮ系列発生器を制御する鍵であり、例えば１秒ごとに更新される。これは同じデコーダを共用しても番組ごとに付随して送られてくるので、番組を送出する放送事業者が独自に管理できる。ただし、複数の放送事業者が同じＰＮ系列を利用してスクランブルを行う場合は、これら放送事業者間で共通管理できる方法が必要である。例としては、衛星テレビ放送の音声(Ａモード)４チャンネルのうち、第３、４チャンネルを独立音声番組の有料放送に使用する場合がある。電通技審の答申方式では同じＰＮ系列発生器の出力系列を用い、スクランブルを行う音声部分でゲートを開いて加算する(5.2参照)ので、第３、４チャンネルの放送が別の放送事業者の場合は、K_sの管理はテレビの放送事業者(第１、２チャンネルを使用している放送事業者)側で行うことになる。

(b) K_w(ワーク鍵)

K_s(スクランブル鍵)を電波等外部から容易にアクセスできる伝送媒体を用いて送る場合に暗号化するための鍵である。このK_wは、暗号アルゴリズムの強度や鍵の管理が完全であれば更新する必要はないが、方式としては更新できるようになっており、例えば１月～１年の単位で更新される。K_wは放送事業者(衛星のチャンネル)ごとに変えることができ、放送事業者で独立に管理できる。受信機では複数のK_wを記憶し、いずれかを選択して番組情報やK_sの暗号を復号する。K_wは電波、ＩＣカード等の物理媒体、電話線等の有線伝送媒体で受信機へ送られるが、電波等外部からアクセス可能な媒体で送る場合はK_m(マスタ鍵)で暗号化される。

(4) 秘密であり、放送事業者単独では管理できない部分

(a) K_m(マスタ鍵)

K_m(マスタ鍵)は他の加入者へ送られる情報を窃用したり、内容を改ざんされないようにするために用いられるもので、各有料デコーダに固有にする必要があり、またデコーダ(あるいはセキュリティＩＣ)を交換しない限り一定となる鍵である。各加入者は契約時にデコーダ番号を放送事業者に知らせると、その番号に対応するK_mで暗号化された個別情報(契約内容とK_w)が配付される。このデコーダのＩＤ番号(外部から観測可能)とK_m(秘密)の対応表は秘密に管理する必要がある。この対応表は、(ｉ)デコーダを製造する場合、(ii) 各加入者の契約時

及び更新時に個別情報を送る場合に必要となる。

ここで複数の放送事業者が共通のデコーダで有料サービスを行う場合には、放送事業者が秘密に管理している情報を互いに知る必要があるので、互いに信頼できる鍵管理の機関が必要となり、デコーダの製造もこの機関が管理する必要がある。

この問題は、技術的には図2の暗号モジュールを含むアクセス制御装置部分をＩＣカード等を利用して完全に分離可能とし[5]、これを放送事業者が独立に管理すれば解決することができる。[6]具体的方法としてはＩＣカードや、イギリスでは電磁誘導による非接触素子が用いられている。[7]ただし、全体のシステムとしてのコストの問題、既に別な方式のデコーダで運用されている状況での導入の問題等を考慮する必要がある。

以上、限定受信システムと情報セキュリティに関する問題について一般的な点を述べた。以下の各章では、各部分に分けてやや詳しく述べてみる。（ただし、ここで述べるものは考え方を紹介するために、公表文献から内容をまとめたものであり、現実にそれらの方式で放送されているかは不明である。）

5．信号スクランブル技術

5.1 信号スクランブル技術の概要

信号スクランブル技術は、画像、音声、データ等の対象とする信号の性質によって異なり、それぞれ従来から種々の方式が検討され、実用化されている。スクランブル方式は、信号の秘匿性が高いこと、復元品質の劣化がないこと、不正復元が困難なこと、回路規模・コストが少ないことなどを考慮して選定される。

秘密通信の場合には通信の存在さえも知られないようにする必要があるが、放送の場合には完全に雑音化すると故障と誤解されやすいこと、若干内容が分る方が受信加入が促進されることなどから、必ずしも秘匿性が完全なものが必要とは限らない。また、秘匿度を制御できることが要求される場合もある。

不正復元については、スクランブル方式を長時間変えないでおくと、信号の性質を解析するなどの方法で復元できることがあるので、スクランブルのパラメータを時間とともに変えて安全性を高めることが必要である。従って、パラメータが変更可能か否かが重要な項目になる。ただし、従来のシステムではスクランブル方式が固定されているものも多く、盗視聴の問題に悩まされてきた。

5.2 音声信号のスクランブル技術

放送では復元品質が問題になるが、ディジタル信号に対するスクランブルは劣化なく復元できるので、衛星放送等ではディジタル化された音声のスクランブルに適用することができる。その方式としては、擬似ランダム信号（ＰＮ信号）を連続的に加算する方式が一般的である。受信側では同じＰＮ信号を生成し、受信された信号系列に加算することによって元の音声信号を復元する。

図5は我が国のＢＳ有料方式における音声スクランブルの構成であり、図中のゲートを制御することにより、図6の音声信号伝送フォーマット上でスクランブルを行う音声チャンネルの部分にＰＮ信号が

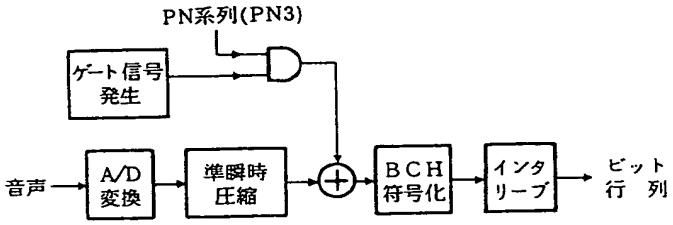


図5　音声信号に対するＰＮ系列の加算位置（ＢＳ有料方式）

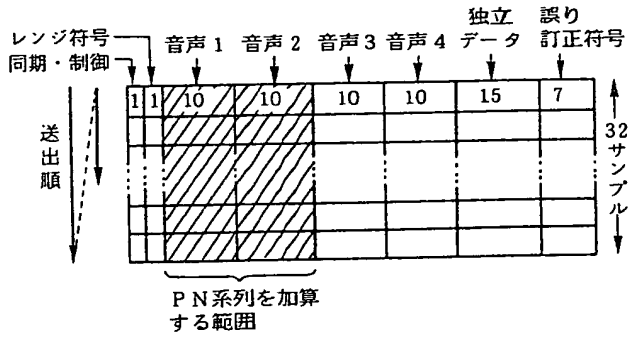


図6　衛星放送音声のビットインタリーブマトリックスとＰＮ系列を加算する範囲（Ａモードで音声1，音声2をスクランブルする場合）

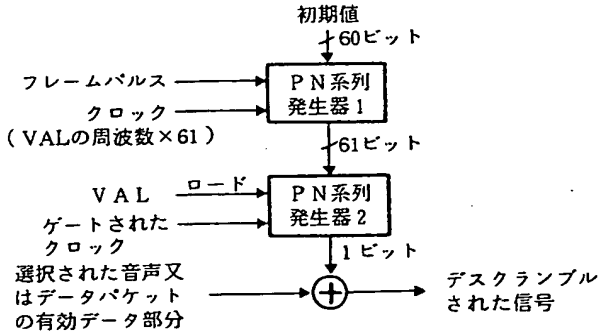


図7　音声又はデータ信号のデスクランブラの構成（ＭＡＣ/パケット方式）

加算される。[11]図7はＥＢＵのＭＡＣ/パケット方式における構成である。[5]

また、アナログ音声の処理として放送に使用された例としては、スペクトル帯域反転(フランスのカナルプルス[8])、妨害波重畳などがある。

5.3 映像信号のスクランブル技術

テレビジョン放送用のスクランブル方式は、大きく振幅方向の処理を行う方式と時間軸方向の処理を行う方式に分けられ、図8のような方式がある。[9]

振幅方向で処理する方式は極性の反転、妨害波の重畳、同期信号の処理、及びこれらの組み合わせが中心であり、ベースバンドで行う他に、ＲＦ信号の段階で処理する方式として実用化されているものが多い。振幅処理による方式は、安全性の点では時間軸処理方式に劣るが、従来の回路技術で比較的簡単に実現でき、コスト的にも有利で、秘匿性も特に問題ないので、これまで多く用いられてきた。

時間軸で処理する方式は、原信号の時間関係を変えて伝送するスクランブル方式であり、例えば、走査線の中で信号の順序を入れ換える、位置をずらす、走査線の順序を入れ換えるなどの方法がある。これらの方式は近年のディジタル回路技術の発達で時間軸の処理が容易になったことから実用化された。ただし、ＡＤ変換器、ＤＡ変換器、画像メモリ等のコストがかかる。

(1) 同期信号を処理する方式

同期信号を抑圧又はレベルを変形するなどして、通常の受像機では同期がかからず流れた画面とする方式であり、最近のＣＡＴＶ用として中心的なスクランブル方式である。水平走査周波数に同期した正弦波を乗算する方法も用いられる。また、安全性を高めるために、同期信号のレベルを数種類設けて切替えることも行われている。受信機で同期信号を正しく再現するためにタイミングやレベルに関する情報が送られるが、その方法としては、例えば音声搬送波を振幅変調する方法がある。

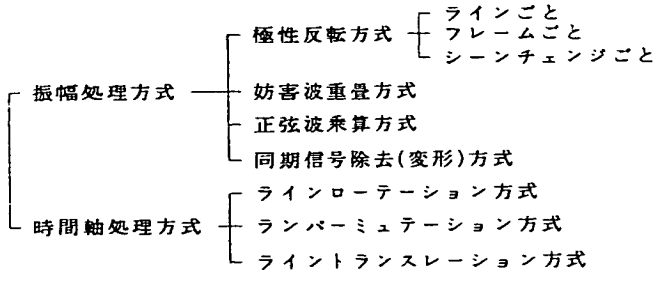


図8　映像信号のスクランブル方式

(2) ラインローテーション方式(走査線内信号切換方式)

各走査線内にカットポイントを設け、その前後を入替えることにより画面を水平方向に乱す方式である。カットポイントの位置を走査線ごとにランダムに変えることにより安全性を得る。多数のスクランブルのパターンを高速に変更することができ、極めて秘匿性が高く、不正復元に強い方式である。

図9はＢＳ有料方式における映像信号のブロック構成を示す。有効伝送画面は186のブロックに分けられ、切断するブロックの境界の番号をＰＮ系列を基に図10の回路で指定することによりスクランブルを行う。また、この指定する数値の範囲を限定することにより、スクランブルの程度の制御(効果制御)を行うことができる。[1]

この方式は伝送路の特性、例えば帯域制限によるリンギング、ディエンファシス特性等による波形ひずみ、同期偏差等の原因により、接続点付近で劣化を生じる場合があり[10]、この対策として、切断部分にオーバーラップを付加して伝送される。この場合の同期信号部分の波形を図11に示す。[1]

ＥＢＵのＭＡＣ/パケット方式では映像信号は輝度信号と色差信号に分けられ、これらと音声及びデータ信号が時分割で伝送される。従って、ラインローテーション方式としては、輝度信号と色差信号を含めてカットポイントを１点設けて前後を入れ替えるシングルカットラインローテーション方式と、輝度信号と色差信号の各々の信号の中にカットポイントを設けてローテーションを行うダブルカットコンポーネントローテーション方式がある。[5][11](図12参照) ダブルカット方式の方が安全性が高いので、ＥＢＵではこの方式を推奨している。[12]

ハイビジョン放送のスクランブルは、伝送信号のＭＵＳＥ信号に対して行うのが適当であり、この場合も輝度信号と色差信号が時分割で伝送される。従って、カットポイントを各走査線に１点設ける１－CUT方式と輝度信号、色差信号の各々に設ける２－CUT方式が可能である。[13]ＭＵＳＥ信号はサンプル値で伝送されるので、ＮＴＳＣ信号に比べて接続点付近の復元画質の劣化の問題は少ない。

(3) ラインバーミュテーション方式(走査線転移方式)

複数の走査線または１フィールドの中で走査線の順序を入れ替える方式であり、画面が垂直方向で乱

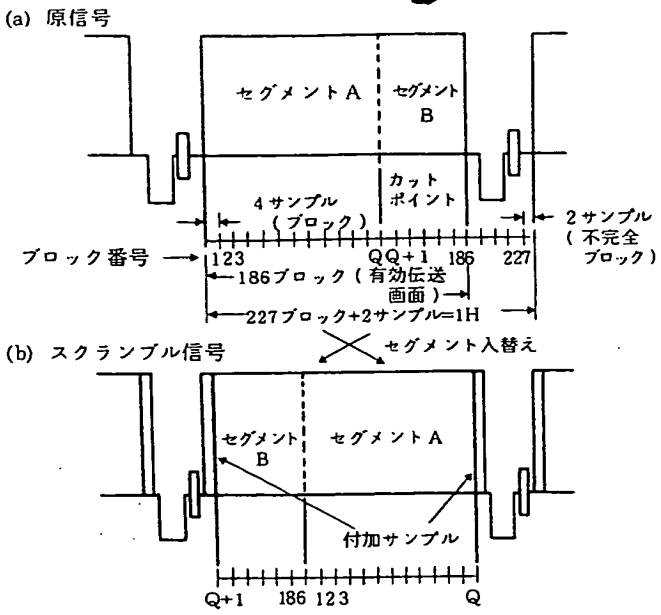


図9　映像信号とブロック構成（ＢＳ有料方式）

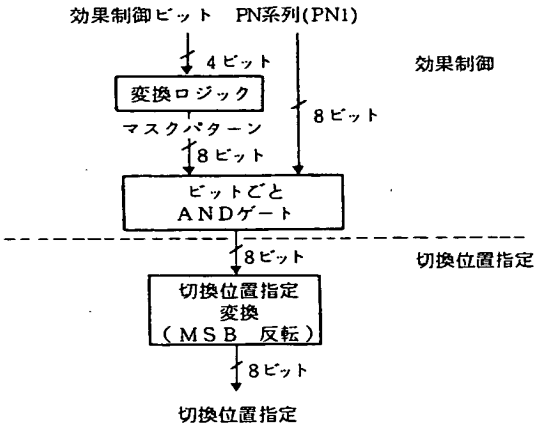


図10　ラインローテーション方式における切換位置指定ロジック（ＢＳ有料方式）

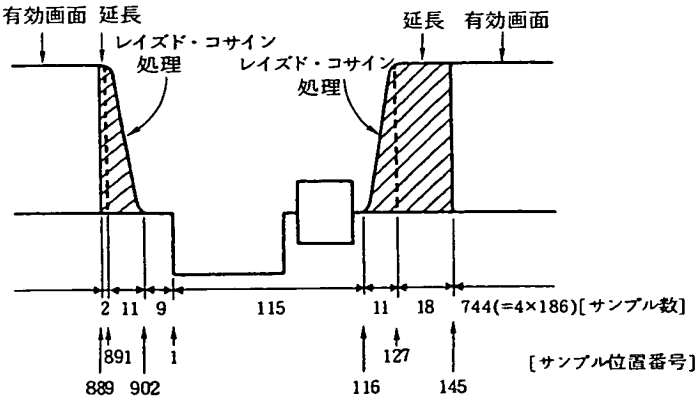


図11　同期信号部分の信号波形（ＢＳ有料方式）

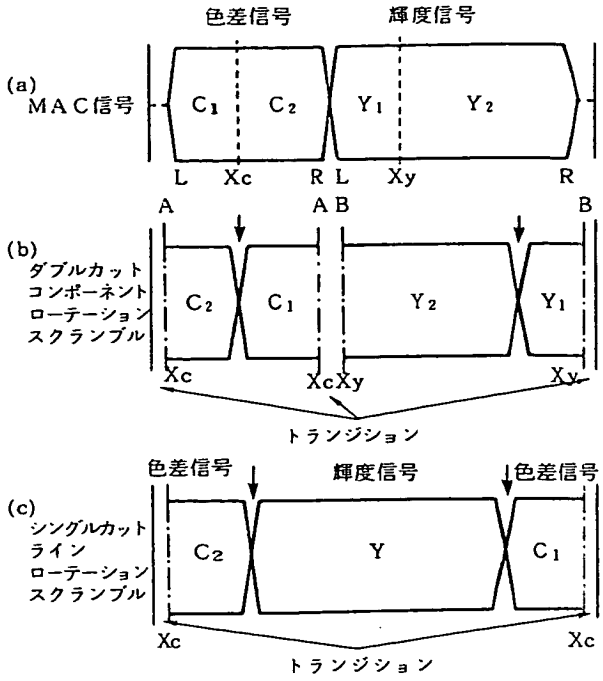


図12　ＭＡＣ/パケット方式の映像スクランブル方式

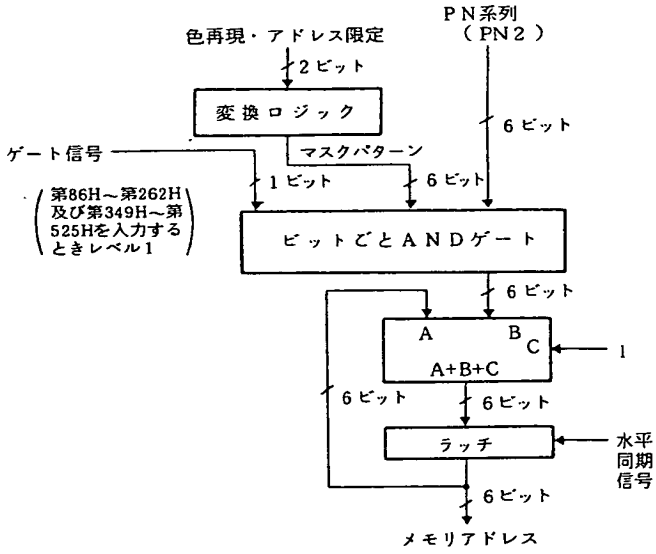


図13　ラインパーミュテーション方式におけるメモリアドレス番号指定ロジック（ＢＳ有料方式）

される。入れ替えるライン数が少ない場合は秘匿性が充分でなく、逆にライン数を増すと画像メモリ量が増え、回路規模、コストが問題になる。ＢＳ有料方式では64ラインの非ブロック化ラインパーミュテーション方式と呼ばれる方式を採用している。[1]この方式は受信機に64ライン分のメモリを持ち、このメモリアドレスをＰＮ系列で直接指定してそのアドレスのメモリ内容を読み出すと同時にそのときに受信されたラインを書き込む方法でデスクランブルを行う方式である。受信機でのメモリアドレス指定回

路を図13に示す。一方、送信側では、予め受信側と同じＰＮ系列を発生させ、受信側でのデスクランブル処理に対応する走査線の入れ替えを１フィールド分のメモリを用いて行うことによりスクランブルを行う。これは受信機のアルゴリズムが極めて簡単になり、放送に適した方式である。

ラインパーミュテーション方式は各走査線内には切断点がないので、ケーブルで伝送するような場合に画質劣化の問題が少ない方式である。

この方式はハイビジョン放送の場合にも適用できる。[13]ただし、走査線数が増えるので秘匿性の点で受信機のラインメモリを増やすことが必要である。

(4) ラインドランスレーション方式

１走査線または複数の走査線をまとめて同期信号の部分の範囲で映像信号をランダムにずらす方式であり、映像がラインごとにずれて見えにくくなる。地上波のテレビの複合信号に適用した例や、ＭＡＣ信号に適用した例がある。[11][14]ＭＡＣ方式の場合は水平同期期間に音声やデータ信号が含まれるので、これらの時間幅をラインごとにランダムに変えることによりスクランブルを行う(図14)。この方式では１走査線内の映像信号は連続しているので、シフトレジスタなどで処理がしやすく、画質劣化を少なくできる利点がある。

5.4 データ信号のスクランブル技術

データ信号を暗号化する方法としては、ディジタル信号系列にＰＮ信号系列を加算する方式(ストリームサイファ方式)と、ディジタル信号系列をある長さのブロックに区切り、そのブロックを暗号化する方式(ブロックサイファ方式)とに大きく分けられる。放送の分野では、テレテキストやデータ放送の限定受信方式が行なわれているが[15]、その方式は、ストリームサイファ方式(ただし、バイト単位の処理)が一般的である。

6．ＰＮ信号系列発生器

スクランブル方式をＰＮ系列で制御する場合、スクランブルされた放送信号の一部とそれらの原信号との対応関係が分ると、作用しているＰＮ系列が分り、スクランブル信号の解読が可能になる。いまＰＮ系列が最も基本的な n段の線形フィードバックシフトレジスタのみで生成されているとすれば、そのＰＮ系列の内の連続２n ビット分が知られると全系列が分るという性質がある。放送信号には原信号が予測できる部分がかなりあるので、例えば、ＰＮ系列発生器を非線形化して出力系列を調べただけでは発生器のパラメータが分らないようにするなどの対策が必要である。この方法の例を図15、図16に示す。

7．関連情報の伝送

7.1 関連情報の伝送媒体の種類と特徴

(a) 電波

１件分の情報量は小さいが、高速で送ることができ、番組の進行に合わせて制御を行うための番組情報の伝送には必須である。第三者が容易にアクセスできるので暗号化が必要であり、また、伝送誤りの対策として再送等の技術が必要である。電波で個別情報を送る場合を「電波アドレッシング」と呼ぶ。

(b) カード等の物理媒体

１件当たりの情報量は多くとれるが、郵送、販売等の流通コストがかかる。ＩＣカードの場合は、データを放送局側へ戻す双方向性の機能を持たせることが容易となる。ＩＣカードを取り入れると、有料

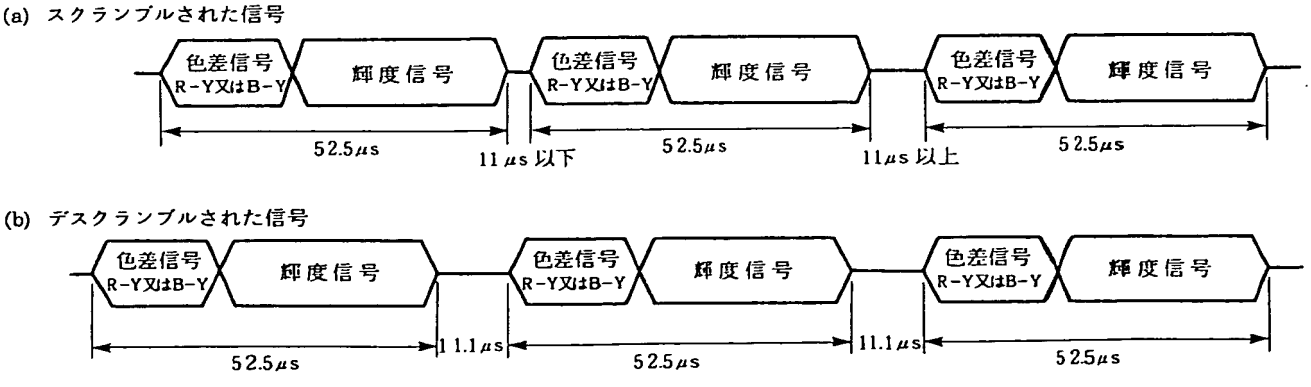


図14　ラインドランスレーション　スクランブル方式（帰線期間の時間は擬似ランダムに変化するが、フィールド間で平均した値は一定）

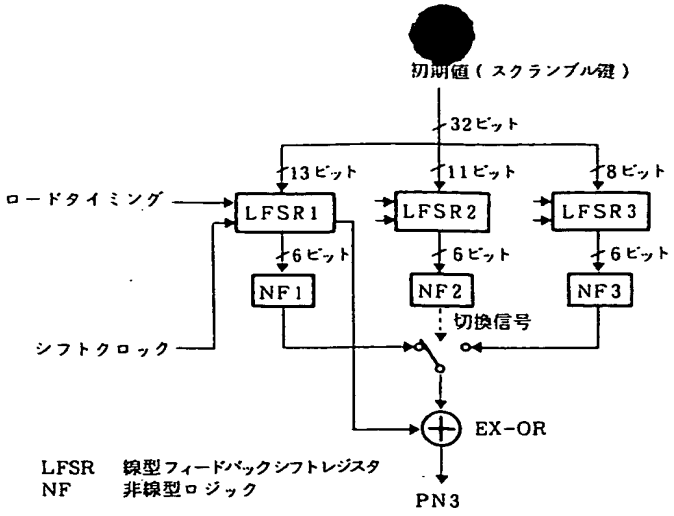


図15 ＰＮ系列発生ロジック[1]（ＢＳ有料方式音声スクランブル用．映像も同様．）

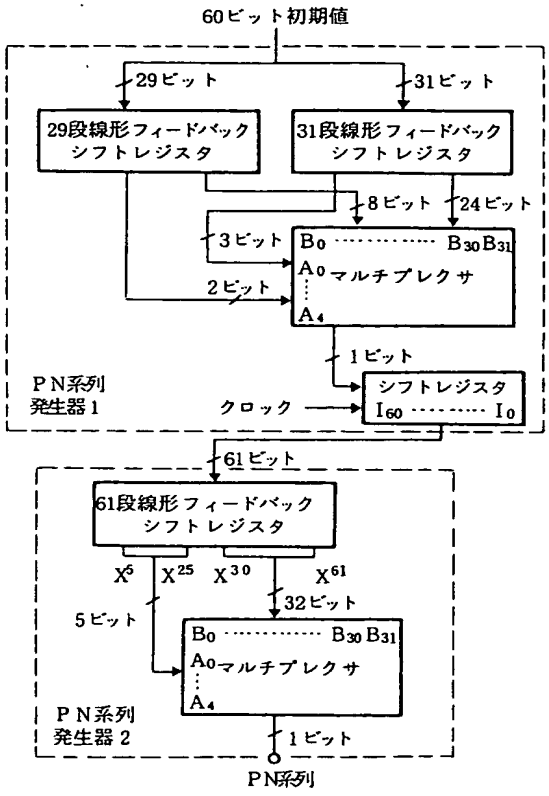


図16 音声/データデスクランブラ用ＰＮ系列発生器の構成[5]（ＭＡＣ/パケット方式）

放送に関わる種々の機能が実現できる。[15]

(c) 電話線

並列伝送を行えば比較的短時間に大量の情報が送れ、双方向性の機能も可能である。ただし、話中で伝わらないことなどへの対策が必要である。

7.2 個別情報の伝送技術

関連情報の伝送技術の点で見ると、番組情報の場合は、実時間で正しく制御するために伝送誤りに対する対策が重要である。一方、個別情報の場合は各加入者に個別に送る必要があることから、大量の情報を送るための技術、また契約内容を改ざんされないための技術などが重要となる。

ＢＳ有料方式の個別情報では、デコーダＩＤに32ビット設け、56ビットのワーク鍵の他に契約内容として各人（１パケット）当り68ビットの情報を送ることができる。[1]衛星放送のデータチャンネルの伝送容量の一部32kb/s分を使うとすれば、毎秒約100件分（１日約900万件、１ケ月約2億6000万件）の情報を送ることができる。１ケ月程度の更新周期であれば各々何回か再送することが可能である。

ところで、ＥＢＵでは電波による鍵の配付に必要な時間を減らすため、共有鍵暗号法を提案している。この方式では図17のような構成のブロックを送る。我が国のワーク鍵に相当する56ビットの補助鍵とモード、共有アドレスの合計84ビットが共有で、アドレス以外の部分が共有配付鍵Ｄで暗号化されて送られる。各加入者に個別の情報は12ビットであり、ベーシックサービスの加入・非加入を示すのであれば12サービス、ティアサービスでは６、ペイパービューでは12ビットで表現した金額のいずれかを送ることができる。これらの23人分が一つのブロックで送られる。

このとき、あるグループの中の加入者が盗聴者と判明した場合に、その鍵を除去するために、受信機の暗号回路に２種類の秘密鍵、すなわち、上記の共有の配付鍵Ｄと加入者ごとに異なる個別鍵Ｕを記憶しておく。盗聴者が判明したときには、そのグループの中の盗聴者以外の人に対して新たなグループ鍵Ｄを各人の個別鍵Ｕで順次暗号化して送る。この作業は能率は悪いが送るべき機会と加入者の数は少ないので問題にならない。

個別情報の内容の改ざんに関しては、ＢＳ有料方式では20ビットの改ざん検出のためのビットが用意されている。[1]また、ＭＡＣ/パケット方式のシステム例では、ペイパービューの前払金の金額を暗号

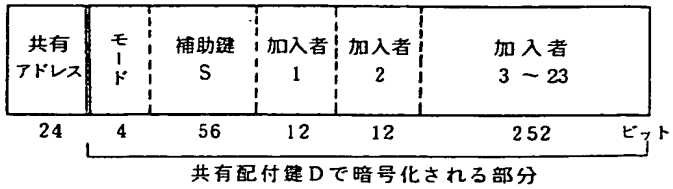


図17 共有発効ブロックの構成（ＭＡＣ/パケット方式）

化して送ると、鍵が異なっていても何等かの値を持って受かることから、予め送ってある補助鍵などと組み合わせて認証することが行われている。[3][5]

8．暗号方式

関連情報を伝送する際に使用される暗号方式、暗号アルゴリズムについては、前述したように我が国のＢＳ有料方式では定められていない。海外のシステムにおいてもほとんど報告はない。ただし、ＥＢＵのＭＡＣ/パケット方式の仕様の中には参考例として図18のような暗号方式が提案されている。[5]

ここで、64ビットの秘密の初期状態Ｉは全てに共通かつ一定で、暗号化及び復号の最初のラウンドにレジスタRにロードされる。スイッチは暗号化のとき e、復号のとき d、の位置におかれる。このアルゴリズムは可変長であり、Ｍバイトの平文(暗号文)をＡレジスタに置き、本アルゴリズムを適当な回数繰り返した後のＢレジスタの内容が暗号文(平文)である。１バイトずつ処理し、全文がＢレジスタへ移ったときを１ラウンドとするとき、暗号文をランダム化するには少なくとも３ラウンド(仕様では８ラウンド)の処理が必要である。図18の一方向性関数の例を図19に示す。ルックアップテーブル(LUT)はランダムな０と１の表であり、全て共通である。

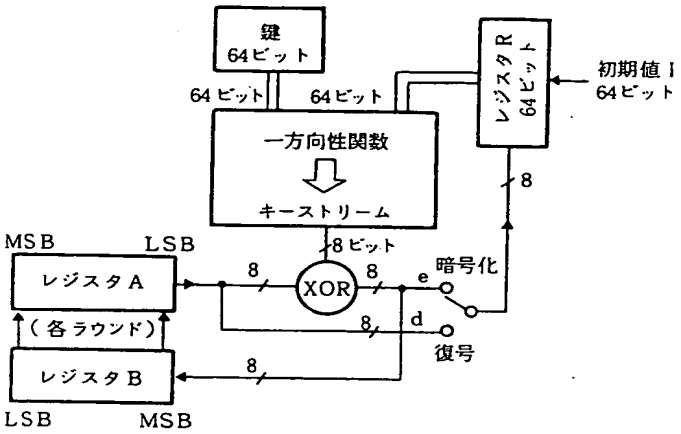


図18　可変長暗号化アルゴリズム

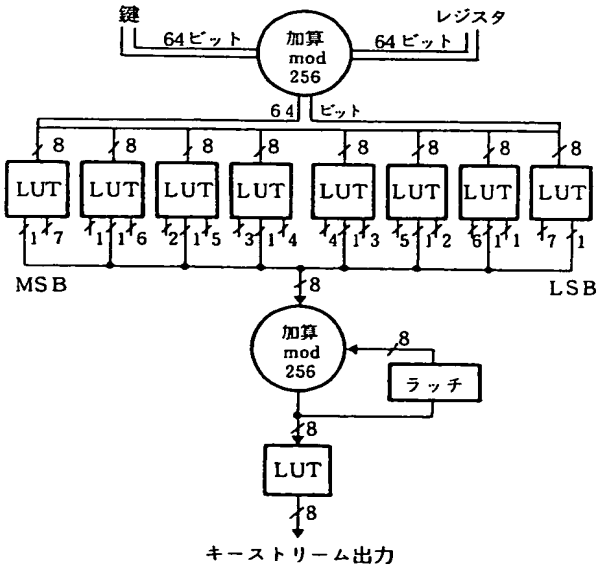


図19　一方向性関数の例

9．むすび

以上、放送における情報セキュリティ技術についていくつかの点を述べたが、今後種々のサービスが実施されるようになると考えられる。そのシステムを考える際に何かの参考になれば幸いである。

参考文献

(1) 郵政省電気通信技術審議会答申第17号 (昭63.11)

(2) "General Characteristics of a Conditional Access Broadcasting System", CCIR Report 1019 (1986,修正1987)

(3) 難波,"放送における情報セキュリティ", テレビ学会誌, 42, 12, pp.1291－1298 (1988)

(4) 郵政省電気通信技術審議会答申第18号 (昭63.3)

(5) "Specification of the Systems of the MAC/Packet Family", EBU Tech.3258－E (Oct. 1986)

(6) 斉藤,木村,難波,"放送受信機におけるICカード内データ処理の検討", 1989年信学春季全大, B－198

(7) S.M.Edwardson,"A conditional access system for direct broadcasting by satellite", J. of IERE, 55, 11/12, pp.377－385 (Nov/Dec 1985)

(8) "Scrambling television", Electronics & Wireless World, 96, 1638, pp.362－363 (Apr. 1989)

(9) "衛星放送における有料方式の技術的諸問題", 衛星放送制度研究会有料方式専門委員会報告書 (1984.2)

(10) 木村,"ラインローテーション方式における復元画質に関する検討", 信学会画像工学研究会資料, IE86－60 (1986.9)

(11) "Satellite Transmission of Multiplexed Analogue Component (MAC) Vision Signals" CCIR Report 1074 (1986)

(12) "The Adoption of One Picture Scrambling Method", EBU Technical Recommendation R35 (1985)

(13) 木村,斉藤,難波,吉野,"ハイビジョン放送信号の伝送に関する一検討", 昭63信学春季全大, B－250

(14) J.D.Lowry,"B－MAC: An optimum format for satellite television transmission", SMPTE J., pp.1034－1043 (Nov.1984)

(15) 松本,加藤,今井,"有料放送に適したアクセス制御方式の提案", 信学会情報理論研究会資料 IT87－55 (1987.9)